UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/655,372	09/05/2003	Masanao Sakai	053969-0157	8586

22428 7590 04/23/2010

FOLEY AND LARDNER LLP
SUITE 500
3000 K STREET NW
WASHINGTON, DC 20007

EXAMINER	
PAN, JOSEPH T	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
04/23/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/655,372	SAKAI, MASANAO	
	Examiner	Art Unit	
	JOSEPH PAN	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 February 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-8,10-13,15,17,18,20,21,23-26,28-30 and 32-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *,3-8,10-13,15,17,18,20,21,23-26,28-30 and 32-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's response filed on February 5, 2010 has been fully considered. Claims 14, 19 and 27 have been canceled. New Claim 36 has been added. Claims 1, 3-8, 10-13, 15, 17-18, 20-21, 23-26, 28-30, and 32-36 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 3-8, 10-13, 15, 17-18, 20-21, 23-26, 28-30, and 32-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arrow et al. (U.S. Patent No. 6,175,917 B1), hereinafter "Arrow", in view of Sullenberger et al. (U.S. Patent No. 7,447,901 B1), hereinafter "Sullengerger".

Referring to claim 1:

i. Arrow teaches:

A network comprising:

IP processing apparatuses, which use an IP (Internet Protocol) for encrypting and authenticating communications via the Internet between two different centers (see figure 1, elements 115, 125, 135, 145, 155; and column 6, line 61, through column 7, line 7, of Arrow); and

an IP setting apparatus, which manages IP settings of the IP processing apparatuses (see figure 1, element 160 'VPN management station'; figure 13, elements 1314 "define access control rules", 1316 "define address translation rules"; and column 15, line 69, through column 16, line 15, of Arrow);

wherein in response to receiving a request from a first IP processing apparatus to communicate with a second IP processing apparatus, the second IP setting apparatus transmits a response (see column 7, lines 26-45, of Arrow).

Arrow discloses IP protocol and IP packets (see column 6, lines 51-54 of Arrow). However, Arrow does not specifically mention the IPsec (Internet Protocol security protocol).

Arrow discloses that the VPN management unit issues a request to a VPN unit for configuration (see column 12, lines 22-25 'configuration module 710 of operating system 116 manages the configuration of VPN unit 115 in response to configuration requests or commands from VPN management station 160.', of Arrow, emphasis added). However, Arrow does not specifically mention that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit.

Arrow discloses that the IP setting apparatus transmits encryption keys to the first and second IP process apparatuses to be used to encrypt and authenticate IP communications between the first and second process apparatuses (see column 11, lines 27-34, of Arrow). However, Arrow does not explicitly disclose the common encryption key.

ii. Sullenberger teaches a method for establishing a dynamic multipoint encryption virtual private network, wherein Sullenberger that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit to dynamically establish an encrypted virtual private network (see figure 1; column 7, line 63 to column 8, line 3; and column 10, lines 38-51, of Sullenberger).

Sullenberger further discloses the IPsec protocol (see column 1, lines 50-59, of Sullenberger), and the common encryption key (see column 2, lines 24-29; and column 7, lines 44-47, of Sullenberger).

iii. The ordinary skilled person would have been motivated to have applied the teaching of Sullenberger into the system of Arrow such that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit and dynamically establish an encrypted virtual private network, because Arrow teaches "VPN management station 160 controls VPN units 115, 125 and 135 through commands and configuration information transmitted to the respective VPN unit through public network 100." (see column 6, lines 31-34, of Arrow, emphasis added). Sullenberger teaches "The invention relates more specifically to a method and apparatus for establishing a **dynamic** multipoint encrypted virtual private network (VPN)." (see column 1, lines 19-21, of Sullenberger, emphasis added). Therefore, Sullenberger's teaching could enhance Arrow's system.

Referring to claims 3-4, 10-11, 16, 23-24, 29:

Arrow and Sullenberger teach the claimed subject matter: a network (see claim 1 above). They further disclose transmitting messages between IPsec setting server apparatus and IPsec processing apparatus (see column 9, lines 19-22 of Arrow).

Referring to claims 5, 12, 25:

Arrow and Sullenberger teach the claimed subject matter: a network (see claim 1 above). They further disclose generating SA (Security Association) parameters (see figure 13, element 1310 'define VPN parameters'; and column 15, lines 52-54 of Arrow).

Referring to claims 6, 13, 26:

Arrow and Sullenberger teach the claimed subject matter: a network (see claim 1 above). They further disclose send a message including the policies and the SA parameters (see figure 13, elements 1310, 1314, 1316; and column 9, lines 19-22 of Arrow).

Referring to claim 7:

Arrow and Sullenberger teach the claimed subject matter: a network (see claim 1 above). They further disclose the keys for encryption and authentication (see column 11, lines 32-34 of Arrow).

Referring to claim 8:

i. Arrow teaches:

An IP setting apparatus managing IP setting of IP processing apparatuses, which use an IP (Internet Protocol) for securing communication via the Internet between two different centers (see figure 1, element 160; figure 13, elements 1314 "define access control rules", 1316 "define address translation rules"; and column 15, line 69, through column 16, line 15, of Arrow),

wherein said IP setting apparatus manages IP policies applied among IP processing apparatus(see figure 1, element 160; figure 13, elements 1314 "define access control rules", 1316 "define address translation rules"; and column 15, line 69, through column 16, line 15 of Arrow), and

wherein said IP setting apparatus includes means for specifying specifies the IP policies of said IP to be applied between a first IP processing apparatus and the second IP processing apparatus (see figure 11, element 1102 'receive request to configure VPN unit'; figure 13, elements 1310 'define VPN parameters', 1314 'define access control rules', 1316 'define address translation rules'; and column 15, line 52-column 16, line 15, of Arrow, emphasis added).

Arrow discloses IP protocol and IP packets (see column 6, lines 51-54 of Arrow). However, Arrow does not specifically mention the IPsec (Internet Protocol security protocol).

Arrow discloses that the VPN management unit issues a request to a VPN unit for configuration (see column 12, lines 22-25 'configuration module 710 of operating system 116 manages the configuration of VPN unit 115 in response to configuration requests or commands from VPN management station 160.', of Arrow, emphasis added). However, Arrow does not specifically mention that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit.

Arrow discloses that the IP setting apparatus transmits encryption keys to the first and second IP process apparatuses to be used to encrypt and authenticate IP communications between the first and second process apparatuses

(see column 11, lines 27-34, of Arrow). However, Arrow does not explicitly disclose the common encryption key.

ii. Sullenberger teaches a method for establishing a dynamic multipoint encryption virtual private network, wherein Sullenberger that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit to dynamically establish an encrypted virtual private network (see figure 1; column 7, line 63 to column 8, line 3; and column 10, lines 38-51, of Sullenberger).

Sullenberger further discloses the IPsec protocol (see column 1, lines 50-59, of Sullenberger), and the common encryption key (see column 2, lines 24-29; and column 7, lines 44-47, of Sullenberger).

iii. The ordinary skilled person would have been motivated to have applied the teaching of Sullenberger into the system of Arrow such that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit and dynamically establish an encrypted virtual private network, because Arrow teaches "VPN management station 160 controls VPN units 115, 125 and 135 through commands and configuration information transmitted to the respective VPN unit through public network 100." (see column 6, lines 31-34, of Arrow, emphasis added). Sullenberger teaches "The invention relates more specifically to a method and apparatus for establishing **a dynamic** multipoint encrypted virtual private network (VPN)." (see column 1, lines 19-21, of Sullenberger, emphasis added). Therefore, Sullenberger's teaching could enhance Arrow's system.

Referring to claim 15:

i. Arrow teaches:

An IP processing apparatus using an IP (Internet Protocol) on the Internet,

wherein said IP processing apparatus receives from an IP setting apparatus managing communication a packet containing the IP to be applied to communication with another IP processing apparatus, determines whether or not to request from the IP setting apparatus a setting for IP communication (see column 4, lines 38-40; column 11, lines 27-30 of Arrow), and

wherein the IP processing apparatus transmits a request to the IP setting apparatus in order to receive from the IP setting apparatus a setting for IP communication (see figure 11, element 1102 'receive request to configure VPN unit'; figure 13, elements 1310 'define VPN parameters', 1314 'define access control rules', 1316 'define address translation rules'; and column 15, line 52-column 16, line 15, of Arrow, emphasis added).

Arrow discloses IP protocol and IP packets (see column 6, lines 51-54 of Arrow). However, Arrow does not specifically mention the IPsec (Internet Protocol security protocol).

Arrow discloses that the VPN management unit issues a request to a VPN unit for configuration (see column 12, lines 22-25 'configuration module 710 of operating system 116 manages the configuration of VPN unit 115 in response to configuration requests or commands from VPN management station 160.', of Arrow, emphasis added). However, Arrow does not specifically mention that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit.

Arrow discloses that the IP setting apparatus transmits encryption keys to the first and second IP process apparatuses to be used to encrypt and authenticate IP communications between the first and second process apparatuses (see column 11, lines 27-34, of Arrow). However, Arrow does not explicitly disclose the common encryption key.

ii. Sullenberger teaches a method for establishing a dynamic multipoint encryption virtual private network, wherein Sullenberger that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit to dynamically establish an encrypted virtual private network (see figure 1; column 7, line 63 to column 8, line 3; and column 10, lines 38-51, of Sullenberger).

Sullenberger further discloses the IPsec protocol (see column 1, lines 50-59, of Sullenberger), and the common encryption key (see column 2, lines 24-29; and column 7, lines 44-47, of Sullenberger).

iii. The ordinary skilled person would have been motivated to have applied the teaching of Sullenberger into the system of Arrow such that a VPN unit

makes a request to the VPN management unit in order to communicate with another VPN unit and dynamically establish an encrypted virtual private network, because Arrow teaches "VPN management station 160 controls VPN units 115, 125 and 135 through commands and configuration information transmitted to the respective VPN unit through public network 100." (see column 6, lines 31-34, of Arrow, emphasis added). Sullenberger teaches "The invention relates more specifically to a method and apparatus for establishing a **dynamic** multipoint encrypted virtual private network (VPN)." (see column 1, lines 19-21, of Sullenberger, emphasis added). Therefore, Sullenberger's teaching could enhance Arrow's system.

Referring to claims 18, 30:

Arrow and Sullenberger teach the claimed subject matter: an IPsec processing apparatus (see claim 15 above). They further disclose the SPD [i.e., Security Policy Database], SAD [i.e., Security Association Database] (see figure 2, elements 203 'IPSec Policy', 124C 'security association', of Sullenberger).

Referring to claims 20, 32:

Arrow and Sullenberger teach the claimed subject matter: an IPsec processing apparatus (see claim 15 above). They further disclose acquiring new setting information (see column 10, lines 41-51 of Arrow).

Referring to claim 21:

i. Arrow teaches:

An IPsec setting method comprising:

receiving from IP processing apparatus a request (see column 14, lines 33-44, of Arrow),

retrieving IP policy rules from memory and generating IP settings parameters based on the content of the request from the IP processing apparatus and the retrieved policy rules (see column 14, lines 33-44, of Arrow); and

transmitting the generated IP settings to the IP processing apparatus (see column 14, lines 33-44, of Arrow).

Arrow discloses IP protocol and IP packets (see column 6, lines 51-54 of Arrow). However, Arrow does not specifically mention the IPsec (Internet Protocol security protocol).

Arrow discloses that the VPN management unit issues a request to a VPN unit for configuration (see column 12, lines 22-25 'configuration module 710 of operating system 116 manages the configuration of VPN unit 115 in response to configuration requests or commands from VPN management station 160.', of Arrow, emphasis added). However, Arrow does not specifically mention that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit.

Arrow discloses that the IP setting apparatus transmits encryption keys to the first and second IP process apparatuses to be used to encrypt and authenticate IP communications between the first and second process apparatuses (see column 11, lines 27-34, of Arrow). However, Arrow does not explicitly disclose the common encryption key.

ii. Sullenberger teaches a method for establishing a dynamic multipoint encryption virtual private network, wherein Sullenberger that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit to dynamically establish an encrypted virtual private network (see figure 1; column 7, line 63 to column 8, line 3; and column 10, lines 38-51, of Sullenberger).

Sullenberger further discloses the IPsec protocol (see column 1, lines 50-59, of Sullenberger), and the common encryption key (see column 2, lines 24-29; and column 7, lines 44-47, of Sullenberger).

iii. The ordinary skilled person would have been motivated to have applied the teaching of Sullenberger into the system of Arrow such that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit and dynamically establish an encrypted virtual private network, because Arrow teaches "VPN management station 160 controls VPN units 115, 125 and 135 through commands and configuration information transmitted to the respective VPN unit through public network 100." (see column 6, lines 31-34, of Arrow, emphasis added). Sullenberger teaches "The invention relates more specifically to a method and

apparatus for establishing a **dynamic** multipoint encrypted virtual private network (VPN)." (see column 1, lines 19-21, of Sullenberger, emphasis added). Therefore, Sullenberger's teaching could enhance Arrow's system.

Referring to claim 28:

Arrow and Sullenberger teach the claimed subject matter: an IPsec setting method (see claim 21 above). They further disclose the inquiry means (see column 14, line 25, of Arrow).

Referring to claims 33-35:

Arrow and Sullenberger teach the claimed subject matter: a network (see claim 1 above). They further discloses transmitting the encryption key to the first and the second IPsec processing apparatus depending on their addresses (see column 9, lines 18-22, of Arrow), and the common encrypt key (see column 2, lines 24-29; and column 7, lines 44-47, of Sullenberger).

Referring to claim 36:

Arrow and Sullenberger teach the claimed subject matter: a network (see claim 1 above). They further discloses the encrypted communication (see column 11, lines 43-45, of Arrow).

Response to Arguments

4. Applicant's arguments, filed on February 5, 2010, have been fully considered but they are not persuasive.

(a) Applicant argues:

"The cited art does not teach the IPsec setting apparatus transmits a common encryption key to the first and second IPsec processing apparatuses." (see page 10, 2nd paragraph)

Examiner maintains:

Arrow further discloses "In state 1310, the system manager defines VPN parameters for authentication, encryption [i.e., the encryption keys], and compression functions to be associated with a newly created VPN." (see column 15, lines 52-54, of Arrow, emphasis added). Therefore, Arrow disclose that the VPN management station [i.e., the IPsec setting apparatus] defines encryption keys for a VPN unit [i.e., the IPsec processing apparatus].

Arrow discloses "RSA module 722 provides public key/private key security functions, including exchanging of certificates for authentication functions with remote entities. Among its other functions, RSA module 722 [i.e., in VPN unit] supports management of **encryption keys** and loading of configuration information into VPN unit 115 **from VPN management station** 160 (from FIG. 1). To this end, RSA module 722 communicates with key management module 738, which itself communicates with VPN processor 718. Key management module 738 sets up keys for encryption and authentication functions." (see column 11, lines 27-34, of Arrow, emphasis added). Therefore, Arrow disclose that VPN management station [i.e., the IPsec setting apparatus] transmits the encryption keys to a VPN unit [i.e., the IPsec processing apparatus].

On the other hand, Sullenberger discloses "Currently IPsec VPN networks are established using point-to-point links among routers or switches that participate in the VPNs. This is a natural way to set up encrypted networks since encryption involves establishing a shared secret [i.e., the common encryption key] between the two endpoints so that each end can decrypt what the other end has encrypted. The most efficient way to manage larger and larger collections of these point-to-point links is to arrange them into hub-and-spoke networks." (see column 2, lines 24-29, of Sullenberger, emphasis added). Therefore, Sullenberger discloses using the common encryption key between the endpoints.

Thus the combination of Arrow and Sullenberger disclose that the IPsec setting apparatus transmits a common encryption key to the first and second IPsec processing apparatuses, such as claimed.

(b) Applicant argues:

"Nor does the cited art teach or suggest an IPsec setting apparatus, in response to receiving from a first IP processing apparatus a request to communicate with a second IPsec processing apparatus, issuing a request to and receiving a response from the second IPsec processing apparatus." (see page 10, 3rd paragraph)

Examiner maintains:

Arrow discloses "As described above, configuration module 710 of operating system 116 [i.e., the VPN unit] manages the configuration of VPN unit 115 in response to configuration requests or commands from VPN management station 160." (see column 12, lines 22-25, of Arrow). Therefore, Arrow discloses that VPN management station [i.e., the IPsec setting apparatus] transmits requests or commands to VPN units [i.e., the IPsec processing apparatus] for configuration, such as configuring encryption keys. However, Arrow does not explicitly disclose that a VPN unit sends a request to the VPN management station in order to communicate with another VPN unit.

On the hand, Sullenberger discloses "The process described dynamically establishes a secure VPN by generating an encryption state for network traffic over a VPN link in response to notification of a virtual address-to-real address mapping. It is further dynamic with respect to spoke-to-spoke VPN links, in that network traffic between two spokes can trigger generation of an encryption state and a security association among the two spokes, via NHRP resolution **requests** and **replies** between **spoke routers** and their **associated NHS**. Therefore, significantly, a statically configured full mesh network is unnecessary. Note that hub-to-spoke links are normally more lasting than spoke-to-spoke links due to the repetitive dynamic routing protocol traffic and NHRP registration and resolution traffic between a hub router and its related spoke routers." (see column 10, lines 38-51, of Sullenberger). Therefore, Sullenberger discloses that a VPN unit sends a request to the VPN management station in order to communicate with another VPN unit.

Thus, the combination of Arrow and Sullenberger disclose an IPsec setting apparatus, in response to receiving from a first IP processing apparatus a request to

communicate with a second IPsec processing apparatus, issuing a request to and receiving a response from the second IPsec processing apparatus, such as claimed.

(c) Applicant argues:

"then the cited art also does not teach or suggest the claim limitation, "upon receiving a reply to the request from the second IPsec processing apparatus the IPsec setting apparatus transmits a common encryption key to the first and second IPsec process apparatuses to be used to encrypt and authenticate IPsec communications between the first and second process apparatuses."." (see page 11, 2nd paragraph)

Examiner maintains:

The combination of Arrow and Sullenberger disclose "upon receiving a reply to the request from the second IPsec processing apparatus the IPsec setting apparatus transmits a common encryption key to the first and second IPsec process apparatuses to be used to encrypt and authenticate IPsec communications between the first and second process apparatuses.", such as claimed (see (a) & (b) above).

Conclusion

5. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph Pan whose telephone number is 571-272-5987.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Joseph Pan
April 16, 2010
/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435